

Kundens IT-miljø

Indholdsfortegnelse

1.	Kundens it-miljø.....	3
1.1.	Kundens it-strategi og standarder	3
1.1.1.	IT-Strategi.....	3
1.1.2.	Standarder.....	3
1	Den fysiske infrastruktur.....	3
2	Den logiske infrastruktur	4
3	Administrativt netværks standarder.....	5
4	Teknisk Netværks standarder	7
5	Standarder for lokalnetværk.....	7
6	Standarder for Webplatforme.....	7
7	Standarder for tjenesterne DNS, DHCP, SMTP, NTP.....	8
8	Standarder for perimetersikkerhed	8
1.1.3.	IT-Sikkerhed	9
1.2.	Kundens systemer	9
1.2.1.	Systemlandskab.....	9
1	Administrativt Netværk	9
1.3.	Datakommunikation	10
1.4.	Udstyr lokaliseret hos Kunden eller tredjemand.....	11
1.4.1.	Servermiljø	11
1.4.2.	Clientmiljø	12

1. Kundens it-miljø

I nærværende afsnit har Kunden beskrevet sit eksisterende og planlagte it-miljø, eller de dele heraf, som Kunden anser for relevante for Leverandøren i forbindelse med levering af ydelsen til Kunden, f.eks. ved specialudvikling.

1.1. Kundens it-strategi og standarder

1.1.1. IT-Strategi

Aarhus kommunes har de sidste 18 år målrettet outsourcet sin IT-drift på centralt fastlagte aftalegrundlag, samtidigt med at afdelingernes lokale driftsenheder i samme periode er reduceret fra 21 til 0.

Aarhus kommune anskaffer i dag som udgangspunkt IT-tjenesteydelser, software- og hardwareleverancer samt IT-driftsydelser gennem centralt fastlagte udbud, men varetager også et antal infrastrukturelle IT-driftsopgaver i den centrale IT-funktion, herunder desk-top management og Print.

De centrale, interne IT-funktioner er således fokuseret på fælles digitalisering, support, leverancestyring og infrastrukturudvikling.

De decentrale interne IT-funktioner er fokuseret på afdelingsspecifik digitalisering og produktspecifik support af fagsystemer.

1.1.2. Standarder

1 Den fysiske infrastruktur

Aarhus kommune ejer sin egen CISCO-baserede fiberinfrastruktur, der forbinder de ca. 1.400 lokationer igennem 53 POP skabe placeret på 10 fiberringe, der igen er forbundet til en backbone med tre redundante knudepunkter. Hertil ca. 70 mindre lokationer opkoblet med ADSL linjer og TDC MPLS.

Alle lokationer kan tilbydes alle tjenester og alle netværk igennem denne infrastruktur.

Hele infrastrukturen er i 2015 opgraderet til ny teknologi fra Cisco, og har derfor den kapacitet der skal til. Core kapaciteten er p.t. 2*10 Gbit/s og kan udvides til 2*40 Gbit/s.

Lokationer er tilsluttet Core med 1 Gbit/s, større lokationer med 10Gbit/s.

Eksterne driftsoperatører er tilsluttet infrastrukturen, enten direkte via kommercielle fiberforbindelser fra TDC, Nianet eller GlobalConnect, med TDC MPLS forbindelser eller med PtP VPN over Internettet. En særstatus har KMD, der er tilsluttet via en proprietær VPN teknologi.

Operatører på WAN infrastrukturen er p.t. :

- TDC / NetDesign : Fysisk fiber

-
- Atea / Axxess : MAN, WAN, FW, DHCP, NTP, Peering
 - TDC: ISP – kapaciteten er p.t. 10 Gbit/s
 - Telefoni og bylinjer: Telenor

2 Den logiske infrastruktur

Aarhus kommunes netværk er opdelt i et antal VRF'er, - der kun har forbindelse med hinanden igennem Firewallregler. Så selvom to VRF'er deler fysisk infrastruktur, er de logisk kun forbundet til hinanden igennem Firewallens regler.

Imellem Internet og VRF'erne er etableret en DMZ, hvor ressourcer kan tilgås udefra igennem Firewallen på tildelte public IP-adresser, og hvor ressourcerne i DMZ kan få regelbaseret ip-specifik adgang til ressourcer i de interne VRF'er.

De mest betydende VRF'er er:

- Administrativt netværk

Fælles for hele organisationen. Tilbyder adgang til servere og platforme til alle administrative formål, herunder behandling og opbevaring af følsomme data. Anvendes af domænepc'er og domæneservere samt managed mobilt udstyr via VPN. Der er som udgangspunkt ikke adgang til administrativt netværks ressourcer fra andre VRF'er.

- Teknisk Netværk

Fælles for hele organisationen. Anvendes til bygningstekniske formål, herunder eksempelvis klimastyring, anden proceskontrol, døråbningssystemer, alarmer og videoovervågning. Netværkets ressourcer er som udgangspunkt synlige fra administrativt netværk, - mens administrativt netværks ressourcer IKKE er synlige fra Teknisk Netværk.

- Pædagogisk netværk

Anvendes af magistratsafdelingen for Børn og Unge til undervisningsrelaterede formål på Skoler. Der er som udgangspunkt ikke adgang til Pædagogisk netværk fra andre VRF'er.

- "Home" netværk

Fælles for hele organisationen. Tilbyder en simpel, trådløs internetforbindelse til udstyr, der via 802.1x teknologi og produktet CISCO ISE er logget på med brugercredentials fra et kommunalt AD, specifikt oprettede brugercredentials fra en internt vedligeholdt LDAP, eller en MAC-adresse der er registreret på en bruger fra den internt vedligeholdte LDAP. Der er ikke adgang til ressourcer i andre VRF'er fra "Home"net og ingen tjenester tilbydes udover internetadgangen.

-
- Publikumsnetværket

Anvendes af Magistratsafdelingen for Kultur og Borgerservice til borgeres adgang til Internettet fra stationære desktops i Bibliotekerne.

- Gæstenet "SmartAarhus"/"Eduroam"

Anvendes af kommunens gæster, der kan få etableret en simpel, trådløs internetforbindelse mod indtastning af credentials (NemID, SMS kode til mobiltelefon eller lånerkort/sygesikringsbevis). Ingen tjenester tilbydes udover Internetadgangen.

3 Administrativt netværks standarder

Directory og rettighedsstyring

Der anvendes Microsoft AD 2012 med 5 DC'er, heraf 2 i eksternt site hos driftsoperatør på Sharepoint 2013 miljøet.

Digitale medarbejdersignaturer for 4-5.000 ansatte i Aarhus kommune administreres og deployeres med "Signaturcentralen" leveret af Signaturgruppen.

Et internt udviklet register, "BrugerIDdatabasen" fungerer kombineret med Microsoft ADFS tjenester som identitets "broker" imellem det administrative netværks AD, NemID, KMD's Novellsystemer (OPUS), Mainframemiljøet m.v. Man kan populært sagt via NemID's CPR-nummer "veksle" en brugers identitet fra et directory til et andet.

ADFS tjenesten er public tilgængelig, og eksterne systemer kan derfor umiddelbart bringes til at anvende credentials fra Aarhus kommunes interne directories, hvis de kan anvende den returnerede SAML-token fra AAK's ADFS.

Desktop

Alle desktops er managed med Microsoft SCCM. Applikationer deployeres som MSI installationspakker med silent/unattended installation.

Antivirus er "Kaspersky".

OS er Win 10 Pro.

Der er på administrativt netværk ca. 4.000 bærbare af fabrikat Lenovo og ca. 8.000 stationære af fabrikat HP. Porteføljen er konsolideret på forholdsvist få modeltyper, da al arbejdspladshardware er anskaffet inden for de seneste fire år. Der er i 2018 indgået ny aftale på leverance af desktops, hvor produktserien på bærbare er HP. Der vil derfor i en årrække fremover være såvel Lenovo som HP bærbare i produktion.

Mobiltelefoner / tablets

Porteføljen er spredt på forskellige platforme, og forventes ikke konsolideret.

Der anvendes ca. 45% iPhone, 45% Android og 10% WinPhone. Tablets til generelt kontorbrug er typisk iPad, mens tablets dedikeret til fagsystemer typisk er Android.

Alle mobiltelefoner og tablets er underlagt device management og deployering baseret på Microsoft Intune deployering.

SIM-kort leveres af én Teleoperatør på indgået aftale herom, - p.t. ”Telenor”. SIM-kort anvender teleoperatørens APN til Internetforbindelse.

Mobile enheder kan via device management udstyres med Cisco AnyConnect Klient og et brugerspecifikt certifikat. Herved kan apparatet forbindes til administrativt netværk efter behov.

Print

Ca. 900 Konica-Minolta Multifunktionsprintere, der er managed med Konica-Minoltas produkter hertil, og som understøtter sikker udskrift og follow-me udskrift.

Lokalt tilsluttede printere understøttes ikke.

Applikationsservere

Alle ca. 400 applikationsservere er som udgangspunkt virtualiserede og hostes i et out-sourcet driftsmiljø, - p.t. et VMware miljø driftet hos ATEA.

Der understøttes Win 2008 R2, Win 2012 R2, Win 2016 og RedHat Linux.

Nye servere etableres på platformen Win2016 med mindre der er vægtige argumenter for at fravige dette.

Driftsmiljøet er SPLA licenseret for Operativsystemets vedkommende, mens Microsoft SQL server Std. og Enterprise som udgangspunkt licenseres af Aarhus Kommune selv på særskilt fysisk driftsmiljø hertil.

Herudover hostes et begrænset antal virtualiserede applikationsservere af forskellige applikationstekniske årsager hos andre driftspartnere.

Filsystem

Alle filshares, herunder brugernes homedirectory, afvikles i et DFS-filsystem hos ekstern serverdriftsoperatør. Office 365 OneDrive forventes at erstatte brugernes homedirectory i forhold til opbevaring af personlige data i løbet af 2019.

Kontorplatform

Der anvendes Microsoft Office 365. Der driftsafvikles stadig et antal interne Sharepoint servere på 2007, 2010 og 2013 platformen, men migrering til Sharepoint 365 vil pågå i de kommende år. Al intern drift af Exchange er indstillet og afviklet.

4 Teknisk Netværks standarder

Det nuværende tekniske netværk er etableret for en del år siden, som et sikkerhedsmæssigt lettere "alternativ" til opkobling på det administrative netværk.

Der er p.t ikke produktstandarder for løsninger afviklet på Teknisk Netværk, idet produktvalg som udgangspunkt er sket lokalt i den enkelte institution eller forvaltning. Tilslutning af systemer, leverandører og udstyr til Teknisk Netværk har også været forankret lokalt på den enkelte institution eller hos den tekniske serviceleder i den enkelte bygning.

Derfor er der en flerhed af Klimastyringssystemer, dørlåsesystemer, videoovervågningssystemer m.v. på dette netværk, og der er et begrænset overblik over systemernes anvendelse og konfiguration.

Et nyt Teknisk Netværk er under etablering i 2018, og på dette netværk vil alle nye byggetekniske systemer og deres udstyr blive opkoblet i en change management proces imellem Fælles Service i Aarhus kommune og en byggeteknisk funderet systemejer. Løsninger på det eksisterende Tekniske netværk får lov at fortsætte, men vil i takt med at der indgår changes eller opgraderinger til dem blive udfases til fordel for tilsvarende standardløsninger på det nye tekniske netværk.

Det nye tekniske netværk er lukket VRF, hvor der ikke er adgang fra de øvrige VRF'er i Aarhus kommune, og det opererer bag sin egen, selvstændige firewall.

5 Standarder for lokalnetværk

I kommunens bygninger patches vægstik til specifikke VRF'er i krydsfelter med Cisco switch udstyr.

Aarhus kommune har anskaffet Cisco ISE som standardprodukt til NAC. NAC på trådet opkobling er p.t. kun fuldt implementeret på DOKK1, men implementeres løbende på alle lokationer, - typisk i forbindelse med andre changes på det aktive netværksudstyr. Cisco ISE NAC vil på sigt helt erstatte den nuværende binding af switch porten til et bestemt VRF.

I vid udstrækning er de logiske netværk også tilgængeligt trådløst fra de ca. 8.000 Cisco Access points, der tilbyder et varierende antal SSID'er afhængigt af AP'ets geografiske placering.

Fremadrettet anvendes Cisco ISE / 802.1x til validering af al trådløs opkobling.

I nyt byggeri og større forandringsprojekter vil der blive lagt vægt på dækning med trådløst net, og der vil ikke nødvendigvis være direkte adgang til trådet net fra alle kontorarbejdspladser.

6 Standarder for Webplatforme

Intranet afvikles i Sharepoint 2007. Dokumenthåndteringssystem "e-doc" afvikles i Sharepoint 2010, Collaboration og Projektrum afvikles i Sharepoint 2013/Sharepoint Office 365.

Et nyt Intranet baseret på OpenSource platformen ”Umbraco” er anskaffet, og vil blive implementeret i løbet af 2018.

Aarhus kommunes hjemmeside www.aarhus.dk anvender Sitecore CMS. Et ny hjemmeside baseret på Open Sourceplatformen ”Umbraco” er anskaffet, og vil blive implementeret i løbet af 2018.

Der er dog ingen vedtagne bindende standarder på WEB-området, og der er derfor også et stort antal mindre og fagspecifikke webløsninger på en betragtelig flerhed af afviklingsplatforme og CMS’er.

7 Standarder for tjenesterne DNS, DHCP, SMTP, NTP

Netværksservicen DHCP afvikles centralt og driften varetages af ekstern operatør. Der anvendes så vidt muligt dynamiske IP-adresser.

DNS afvikles på administrativt og pædagogisk netværk af de respektive netværks AD Domaincontrollere, for så vidt angår domænerne egne zoner, - alle andre zoner forwardes til en intern DNS i AAK’s Infrastruktur, hvor interne zoner resolveres internt, og herfra – hvis zonen ikke findes internt – forwardes til Googles DNS.

SMTP for systemer der IKKE anvender Exchange365 tilbydes af AAK’s Postoperatør på en særskilt tjeneste. Aarhus kommune opretter IKKE SPF records for domænet @aarhus.dk til eksterne postoperatører. Skal et system afsende mails der kan SPF checkes, skal de derfor ENTEN være afsendt fra Aarhus Kommunes Microsoft Office 365. – ELLER være afsendt fra Aarhus kommunes interne SMTP tjeneste.

NTP afvikles på intern server. Alle komponenter i AAK infrastruktur skal anvende denne NTP.

8 Standarder for perimetersikkerhed

Firewallteknologien er kontekstbaseret Cisco ASA. Firewallarkitekturen er i 2018 under omlægning, således at der etableres én logisk firewall pr. VRF.

Al udgående trafik fra et VRF NAT’tes til én eller flere public IP for det pågældende VRF.

Udgående trafik fra servere i DMZ NAT’tes til dedikerede Public IP-adresser fra 6 C-klasser registreret som PI til Aarhus kommune. Der anvendes ikke PA IP-adresser fra ISP’en TDC.

Indgående VPN sker med Cisco AnyConnect eller gennem Site-to-site VPN opkoblinger.

Web-proxy håndteres af redundante CitrixNetscaler.

1.1.3. IT-Sikkerhed

Aarhus kommunes IT-Sikkerhedspolitik ligger på [Aarhus kommunes hjemmeside](#).

Den tilhørende IT-sikkerhedshåndbog er baseret på DS484, og kan rekvireres fra Aarhus kommune.

1.2. Kundens systemer

1.2.1. Systemlandskab

1 Administrativt Netværk

For en administrativ medarbejder i Aarhus kommune er systemlandskabet delt i de fælles systemer, og de fagspecifikke systemer.

Fælles systemer er, ud over kontorpakken:

- Journalsystem. (Fujitsu E-doc)

Systemet håndterer på tværs af alle afdelinger journalisering og dokumentation af sager og dokumenter, herunder e-mails. Systemet genererer de offentlige postlister.

Fujitsu e-doc integrerer med Microsoft Office gennem tilføjelsesprogrammer og plug-ins, men har også en webbaseret brugerflade og en APP til mobile devices.

- Mødebooking. (RessourceCentral)

Systemet er indlejret i Microsoft Office gennem tilføjelsesprogrammer og plug-ins.

- Dokumentskabeloner. (dynamictemplate)

Systemet er indlejret i Microsoft Office gennem tilføjelsesprogrammer og plug-ins.

- Sikker e-mail (TietoEnator)

Systemet er indlejret i Microsoft Office gennem tilføjelsesprogrammer og plug-ins.

-
- ERP (KMD OPUS)

Systemet tilgås dels med SAP klient lokalt deployeret til desktoppen, og med browserbaseret brugerflade (KMD Rollebaseret Indgang). Systemet omfatter funktioner til såvel løn- og personaleadministration og økonomistyring.

Herudover er der i den browserbaserede brugerflade og i en egenudviklet APP til Mobile devices adgang til personlig administration af fravær, sygdom og kørsel.

- Intranet (WMdata)

Intranettet er baseret på en platform udviklet i Sharepoint 2007 og anskaffet i 2007 fra daværende WMdata. Den grundlæggende struktur og opbygning er uændret siden. Intranettet har en fælles del, og seks magistratsafdelingsspecifikke dele. Funktionalitet og indhold i den fælles del og de magistratsafdelingsspecifikke dele er delvist overlappende.

Et nyt Intranet baseret op OpenSource platformen ”Umbraco” er anskaffet, og vil blive implementeret i løbet af 2018.

Herudover har en administrativ bruger – helt afhængigt af vedkommendes funktion – adgang til en række fagspecifikke systemer. En del afvikles som client/server med serveren placeret internt i Aarhus kommunes hostede driftsmiljø, andre afvikles som client/server med serveren hostet hos systemleverandøren. Specielt i magistratsafdelingen for Sociale forhold og Beskæftigelse og Magistratsafdelingen for Børn og Unge anvendes en lang række Mainframebaserede systemer, der tilgås med 3270-emulator, - disse systemers antal er dog vigende.

Den administrative bruger anvender i udstrakt grad mobiltelefon og/eller tablet til læsning af mail og opslag i dokumenthåndteringssystemet, mens den strukturerede og planlagte udbredelse af apps, hvis primære funktionalitet ligger på den mobile device, er meget begrænset for den administrative bruger.

1.3. Datakommunikation

Er løsningens servere placeret hos udbyderen af løsningen, skal trafikken krypteres enten med certifikater fra Aarhus kommunes interne PKI, eller med tidssvarende certifikater stillet til rådighed af udbyderen.

Aarhus kommune er fleksibel med hensyn til etablering af lukket datakommunikation med en ekstern driftsudbyder/systemleverandør, og understøtter under forudsætning af indgået Databehandlertale:

- Routning igennem eksisterende kommerciel fiber, - TDC MPLS, Nianet eller GlobalConnect.

-
- Routning igennem en for udbyderens regning etableret ny kommerciel fiber til Aarhus Kommunes infrastruktur (redundant indgang på hhv. Rådhuset og Grøndalsvej 1, Viby.
 - Point to Point VPN over AAK's internetforbindelse.
 - Individuelt tildelt og personlig VPN adgang for medarbejder(e) hos Leverandøren.
 - SSL kommunikation over Internet

1.4. Udstyr lokaliseret hos Kunden eller tredjemand

1.4.1. Servermiljø

Leverandøren kan vælge at tilbyde sin løsning

1. Hostet i Aarhus kommunes driftsmiljø for virtuelle servere, p.t. placeret ved ATEA.

Omkostningen ved hosting i dette miljø afregnes direkte af operatøren med Aarhus kommune, hvorfor denne omkostning som udgangspunkt skal tillægges den tilbudte pris på en given løsning.

Som udgangspunkt vil overdragelse, driftsprøve og performancemålinger skulle udføres på de virtuelle servere, som Leverandøren gennem VPN eller tilsvarende får adgang til at udføre sin systemvedligeholdelse og –installation på.

2. Hostet hos Leverandøren selv, eller ved 3. part på kontrakt med Leverandøren.

Omkostningen ved denne hosting er typisk indregnet i løsningens tilbudte pris.

Som udgangspunkt vil performancemålinger skulle udføres i indgangen til Aarhus kommunes infrastrukturens coremiljø, enten via kommerciel fiber, SSL over Internettet eller Point to Point VPN over Internettet.

3. Gælder alene for nyt Teknisk Netværk:

Option 1 og 2 gælder også for nyt Teknisk Netværk, - men herudover kan leverandøren tilbyde sin løsning opstillet i teknikrum på Aarhus kommunes lokationer. Anvendes denne option, er det dog en forudsætning at leverandøren kan etablere en PtP VPN forbindelse hvorigennem udstyret driftes, - at Aarhus kommune v. Fælles Service Infrastruktur godkender løsningens drifts- og sikkerhedsarkitektur, - samt at Aarhus kommune v. Fælles Service Infrastruktur får administratoradgang til de lokalt opstillede systemkomponenter, så de ved akutte driftshændelser kan deaktiveres eller lukkes ned.

Som udgangspunkt vil overdragelse, driftsprøve og performancemålinger skulle udføres på det lokalt opstillede udstyr.

1.4.2. Clientmiljø

Der henvises til afsnit 2.1.2 / 3. Administrativt netværks standarder - Desktop